ABSTRACT OF THE DISCLOSURE

METHOD AND SYSTEM FOR STEPPING UP TO CERTIFICATE-BASED AUTHENTICATION WITHOUT BREAKING AN EXISTING SSL SESSION

A method is presented for performing authentication operations. When a client requests a resource from a server, a non-certificate-based authentication operation is performed through an SSL (Secure Sockets Layer) session between the server and the client. When the client requests another resource, the server determines to step up to a more restrictive level of authentication, and a certificate-based authentication operation is performed through the SSL session without exiting or renegotiating the SSL session prior to completion of the certificate-based authentication operation. During the certificate-based authentication procedure, an executable module is downloaded to the client from the server through the SSL session, after which the server receives through the SSL session a digital signature that has been generated by the executable module using a digital certificate at the client. In response to successfully verifying the digital signature at the server, the server provides access to a requested resource.